AMENDMENTS TO THE CLAIMS

1-11. (Canceled)

12. (Currently Amended) A method for sending a data packet from a first member of a virtual private network to a second member of the virtual private network comprising the steps of:

receiving a data packet enroute to the second member;

determining if the data packet is being sent between members of the virtual private network, and if so:

determining the packet manipulation rules for packets sent between members of the virtual private network;

forming a secure data packet by executing the packet manipulation rules on the data packet; and

forwarding the secure data packet to the second member of the virtual private network;

wherein said step of determining the packet manipulation rules includes the step of accessing a memory ~~lookup table~~ that maintains information identifying compression and encryption algorithms to be utilized for data packets sent between members of the virtual private network; and

wherein said step of forming a secure data packet includes the steps of encrypting at least a payload portion of the data packet according to the identified encryption algorithm; and compressing at least the payload portion of the data packet according to the compression algorithm identified.

13. (Previously Presented) The method according to claim 12, wherein said compressing step occurs prior to said encrypting step.

14. (Previously Presented) The method according to claim 12, wherein if it is determined that the data packet is not being sent between members of the virtual private network, the data packet is not encrypted.

15. (Previously Presented) The method according to claim 14, wherein if it is determined that the data packet is not being sent between members of the virtual private network, the data packet is not compressed.

16. (Previously Presented) The method according to claim 12, wherein if it is determined that the data packet is not being sent between members of the virtual private network, the data packet is not compressed.

17. (Previously Presented) The method according to claim 12, wherein said receiving step occurs within a virtual private network unit.

18. (Currently Amended) The method according to claim 17, wherein the virtual private network unit is implemented in software running on a computer and the memory is ~~lookup table in~~ located in ~~a memory of~~ the computer.

19. (Previously Presented) The method according to claim 17, wherein the virtual private network unit is implemented in a hardware device placed between a gateway device and the Internet.

20. (Previously Presented) The method according to claim 17, wherein the virtual private network unit is implemented in a hardware device placed between a gateway device and a local area network including the first member of the virtual private network.

21. (Previously Presented) The method according to claim 12, wherein said step of determining that the data packet is being sent between members of the virtual private network includes comparing at least a destination address of the data packet to a list of stored destination addresses.

22. (Currently Amended) The method according to claim 12, wherein the memory ~~lookup table~~ maintains a plurality of different encryption algorithms, each encryption algorithm being associated with a different virtual private network, and wherein different virtual private networks may include one or more common members.

23. (Currently Amended) The method according to claim 12, wherein the memory ~~lookup table~~ also maintains information identifying an authentication algorithm to be utilized for data packets sent between members of the virtual private network; and

wherein if it is determined that the data packet is being sent between members of the virtual private network, authentication information is associated with the data packet according to the identified authentication algorithm.

24. (Currently Amended) A virtual private network unit for sending a data packet from a first member of a virtual private network to a second member of the virtual private network comprising:

an input for receiving a data packet enroute to the second member;

circuitry and software for determining if the data packet is being sent between members of the virtual private network, and if so for:

determining the packet manipulation rules for packets sent between members of the virtual private network; and

forming a secure data packet by executing the packet manipulation rules on the data packet; and

an output for forwarding the secure data packet to the second member of the virtual private network, wherein the packet manipulation rules are stored in a memory ~~lookup table~~ connected to said circuitry and software, and said memory ~~lookup table~~ maintains information identifying compression and encryption algorithms to be utilized for data packets sent between members of the virtual private network, and said circuitry and software forms a secure data packet by encrypting at least a payload portion of the data packet according to the identified encryption algorithm and by compressing at least the payload portion of the data packet according to the compression algorithm identified.

25. (Previously Presented) The virtual private network unit according to claim 24, wherein said circuitry and software compresses the data packet prior to encrypting the data packet.

26. (Previously Presented) The virtual private network unit according to claim 24, wherein if said circuitry and software determines that the data packet is not being sent between members of the virtual private network, said circuitry and software does not encrypt the data packet.

27. (Previously Presented) The virtual private network unit according to claim 26, wherein if said circuitry and software determines that the data packet is not being sent between members of the virtual private network, said circuitry and software does not compress the data packet.

28. (Previously Presented) The virtual private network unit according to claim 24, wherein if said circuitry and software determines that the data packet is not being sent between members of the virtual private network, said circuitry and software does not compress the data packet.

29. (Currently Amended) The virtual private network unit according to claim 24, wherein said circuitry and software are part of a computer and said memory is ~~lookup table in~~ located in ~~a memory of~~ said computer.

30. (Previously Presented) The virtual private network unit according to claim 24, wherein said circuitry and software are implemented in a standalone hardware device placed between a gateway device and the Internet.

31. (Currently Amended) The virtual private network unit according to claim 24, wherein ~~the~~ said circuitry and software are implemented in a standalone hardware device placed between a gateway device and a local area network including the first member of the virtual private network.

32. (New) The method according to claim 12, wherein if it is determined that the data packet is not being sent between members of the virtual private network, the data packet is not sent.

33. (New) The virtual private network unit according to claim 24, wherein if said circuitry and software determines that the data packet is not being sent between members of the virtual private network, said circuitry and software does not send the data packet.

34. (New) The method according to claim 17, wherein the virtual private network unit is implemented in a firewall device.

35. (New) The virtual private network unit according to claim 24, wherein said circuitry and software are part of a firewall device.